UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 21-20264

v.

Hon. Denise Page Hood

YLLI DIDANI,

Defendant.

Mark Bilkovic (P48855)
Timothy P. McDonald
Assistant United States Attorneys
211 W. Fort St., Ste. 2001
Detroit, MI 48226
(313) 226-9623
mark.bilkovic@usdoj.gov
Timothy.mcdonald@usdoj.gov
Attorneys for the United States

Ylli Didani
PRO SE DEFENDANT
FDC Milan
4004 Arkona Road
Milan, MI 48160

Wade G. Fink (P78751)
WADE FINK LAW, P.C.
550 W. Merrill St Suite 100
Birmingham, MI 48009
(248) 712-1054
wade@wadefinklaw.com
Standby Counsel Only

DEFENDANT'S MOTION IN LIMINE
TO EXCLUDE SKYECC EVIDENCE

Defendant Ylli Didani requests that this Court exclude evidence obtained from SkyECC.

Date: January 20, 2025

Respectfully Submitted,

/s/ Ylli Didani (with permission WGF)[1]

PRO SE DEFENDANT
FDC Milan
4004 Arkona Road
Milan, MI 48160

[1] Standby counsel was asked to file the foregoing motion. Counsel had no part in the drafting of the substance of this motion, but assisted in a citation to a news article, as requested, and other formatting and minor corrections for understanding of the reader.

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 21-20264

v.

Hon. Denise Page Hood

YLLI DIDANI,

Defendant.

Mark Bilkovic (P48855)
Timothy P. McDonald
Assistant United States Attorneys
211 W. Fort St., Ste. 2001
Detroit, MI 48226
(313) 226-9623
mark.bilkovic@usdoj.gov
Timothy.mcdonald@usdoj.gov
Attorneys for the United States

Ylli Didani
PRO SE DEFENDANT
FDC Milan
4004 Arkona Road
Milan, MI 48160

Wade G. Fink (P78751)
WADE FINK LAW, P.C.
550 W. Merrill St Suite 100
Birmingham, MI 48009
(248) 712-1054
wade@wadefinklaw.com
Standby Counsel Only

BRIEF IN SUPPORT

Defendant, Ylli Didani, respectfully moves this Court for an order excluding any evidence, testimony, or reference to Sky ECC Communications, including any

intercepted messages, data, or related materials obtained from Sky ECC, from being introduced at trial. In support of this Motion, the Defendant submits the following.

INTRODUCTION

The government intends to introduce evidence of communications obtained through the Sky ECC encrypted messaging platform as part of this case against the Defendant. The Defendant seeks to exclude this evidence on several grounds including the illegality of the seizure, violations of privacy, and lack of authentication. Specifically, the Defendant argues that the unwarranted seizure of this data violates the Fourth Amendment and that the evidence fails to meet the foundational requirements for admissibility under the Federal Rules of Evidence and its introduction would result in unfair prejudice.

Sky Global, a company headquartered in Vancouver, Canada, began developing encrypted Sky ECC phones in 2008. Belgian police began investigating the use of these Sky ECC phones in 2016. In 2018, several law enforcement officers from around the globe, including the US, met and started discussing ways to break the Sky ECC encryption. In 2019, Dutch technicians were able to break the decryption and access live interception and decryption of ALL Sky ECC messages. This effectively opened up the private data to law enforcement of over 170,000 users.

At that time a Dutch magistrate rightfully refused an order to seize full copies of the Sky ECC servers as "it could not be established that the users of Sky ECC

were using the system exclusively for illegal purposes."[2] In finding that because there was no concrete suspicion against individual users, it would be "too far reaching" to grant unconditional permission to search all Sky ECC users.

After this, French investigators using the Dutch technicians decryption started live interception and decryption of ALL Sky ECC messages. Ultimately Dutch police obtained intercepted messages of all incoming and outgoing communications from Sky ECC from France circumventing the Amsterdam Judges decision. France's hack has them sitting on whole servers from Sky ECC containing the private data of citizens across the world this is a massive assault on privacy and human rights. Law enforcement from other nations are now trying to bypass their constitutions and citizens rights by having France cherry pick information on their behalf through theoretical loopholes like MLAT. This is a clear violation of the fourth amendment and should not be allowed.

LEGAL STANDARD FOR ADMISSIBILITY OF EVIDENCE

Under the Federal Rules of Evidence, only relevant evidence is admissible in court Fed. R. Evid. 402. Even if evidence is relevant it may still be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion, or misleading of the jury. Fed. R. Evid. 403.

[2] https://www.computerweekly.com/news/366615638/Ex-boxer-fights-US-government-over-legality-of-Sky-ECC-cryptophone-intercepts

Additionally evidence must be properly authenticated before it can be admitted. Fed. R. Evid. 901. The government bears the burden of establishing a proper foundation for the evidence, including proving that the evidence is what it purports to be and that it was lawfully obtained.

ARGUMENT

A. Sky ECC Evidence Was Obtained in Violation of Constitutional Rights

The Defendant asserts that the Sky ECC evidence was obtained through illegal interception, in violation of the Fourth Amendment. The Fourth Amendment protects against unreasonable searches and seizures, and the government must demonstrate that any search or seizure of electronic communications was conducted with proper legal authorization, such as a valid search warrant.

Lack of a Valid Warrant: If the government obtained access to Sky ECC communications without a valid, court-approved warrant or in violation of applicable law, the evidence obtained through such means must be excluded as the "Fruit of a Poisonous Tree" under Exclusionary Rule principles. The Government in utilizing evidence from France that was obtained through a European Police hacking operation that breaches the constitutional rights of the Defendant. Furthermore, the government waited SIX MONTHS after the defendant was detained and then requested this data from the French authorities using them as virtual agents of the

United States (hiding under the veil of MLAT) so they can circumvent US Law and the constitution.

The Fourth Amendment requires that all searches and seizures of "persons, houses, papers, and effects" be reasonable. U.S. Const. amend. IV. "where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, ...reasonableness generally requires the obtaining of a judicial warrant" supported by probable cause. See *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995). A warrantless search is reasonable "only if it falls within a specific exception to the warrant requirement." See *Riley v. California*, 134 S. Ct. 2473, 2482 (2014). When weighing the reasonableness of a search, court must first decide whether the search was performed to discover evidence of wrongdoing. If the purpose of the search is to perform an ordinary criminal investigation, then law enforcement officers must get a warrant. *Vernonia Sch. Dist.*, 515 U.S. at 653.

This was definitely an ordinary criminal investigation as the defendant was already in custody therefore the government needed a warrant to obtain the Sky ECC data. They knew the manner in which this data was obtained by France would never pass through US Law and had France act on their behalf which is unlawful and a violation of the constitution. Essentially France has a forest full of poisonous trees and the US government placed an order for the tainted fruit. This sets a dangerous

precedence and could result in global food poisoning and the erosion of the constitution.

Violations of Privacy: Sky ECC users have a reasonable expectation to privacy in their encrypted communications. If the government failed to properly comply with procedural safeguards required for accessing private communications, the evidence should be excluded. This mass interception of over 170,000 users was a global fishing expedition without probable cause as there was no reasonable reason to believe all of these users were guilty of criminality.

B. Lack of Authentication and Chain of Custody

The Government is required to authenticate any evidence it seeks to introduce at trial. Under Fed. R. Evid. 901, the Government must establish a chain of custody and prove that the evidence is what it purports to be.

Unverified Source and Possible Tampering: The Government has failed to establish a sufficient chain of custody for the Sky ECC evidence. there is no clear documentation or verification of how the data was obtained, processed or transferred. With the decryption of this data some underlying raw data and "hash values" that would allow experts to check the data provided in evidence and verify it has not been modified is missing. Dutch police developed AI software known as Chat-X that accessed and analyzed intercepted messages this software has not been disclosed and the metadata has not been provided. Its clear the encrypted data could

have been tampered with during the retrieval and subsequent handling. Digital Data is at a significant higher risk of intentional manipulation and alteration. There are concerns about whether the integrity of the evidence has been maintained. Without an adequate foundation, this evidence should not be admitted.

C. Unfair Prejudice and Confusion to the Jury

Even if the Sky ECC data evidence were ruled relevant, it should be excluded under Fed. R. Evid. 403 because its potential for unfair prejudice substantially out weighs its probative value. The jury may be confused or misled by technical evidence related to encrypted communications, especially if the Government cannot fully explain how the messages were intercepted and decoded and since the evidence wasn't intercepted and decoded by this government I fail to see how they can.

Technical Complexity: The jurors may lack the technical knowledge necessary to understand the intricacies of encrypted communications especially when it comes to the process of how that information is decoded and decrypted. This could result in confusion and improper inferences being drawn.

Unfair Prejudice: The introduction of private communications from a secure platform could unfairly prejudice the jury by painting the defendant in a negative light without providing clear and reliable evidence of the Defendants involvement in illegal activity.

D. Sky ECC's Status as a Privacy Platform

The Sky ECC platform is known for its high level of encryption and privacy features, and there is an inherent public policy interest in protecting the privacy of communications conducted over such platforms. Allowing evidence from such sources could set a dangerous precedent for the erosion of privacy rights.

Erosion of Privacy Rights: Admitting evidence obtained through encrypted communication platforms without proper safeguards could lead to chilling effects on digital privacy, violating the constitutional rights of individuals. The manner in which this data was intercepted through the mass interception of over 170,000 users is a blatant violation of those rights because as mentioned there is no reason for the authorities to believe that all the users placed under surveillance were guilty of a crime.

Government's Burden: The government has not sufficiently proven that the data from Sky ECC is lawfully obtained and meets the standards necessary for admissibility

CONCLUSION

For all the reasons set forth above, the Defendant respectfully requests that this Court exclude any evidence, testimony, or references to Sky ECC communications, including any intercepted messages, data, or related materials, from being admitted at trial. The evidences existence is a clear assault on the

constitution as it was unlawfully obtained, lacks proper authentication, and its introduction would set dangerous precedence and be highly prejudicial to the Defendant.

Date: January 20, 2025

Respectfully Submitted,

/s/ Ylli Didani (with permission WGF)

PRO SE DEFENDANT
FDC Milan
4004 Arkona Road
Milan, MI 48160

CERTIFICATE OF SERVICE

On January 20, 2025, standby counsel, who signs below, filed the foregoing using the Court's e-filing system, which will send notice of same to all parties of record. Standby counsel filed this way at the direction of the Clerk's Office regarding Defendant's pro se status and its preference for future filings.

/s/ Wade G. Fink